07/12/01

Docket No. 8X8S.261PA

Data Security Apparatus And Method Therefor

Field of the Invention

The present invention relates to data security systems, and more particularly, to automatic detection for securing electronically displayed data.

Background of the Invention

Image communication systems span a variety of applications. One such application is security monitoring. In many applications, security monitoring involves system control and display functions located at a central station. The central station includes multiple emanating video-communication paths, each path connecting to a remotely-located display camera. Traditionally, the significant expense of security monitoring systems has limited their practicability to larger facilities.

Recent developments in communication standards and compression / decompression techniques have permitted enhanced security-system implementations. One generally-described approach involves using a remote camera that responds to changes in motion or audio as a determining factor for transmitting captured video and audio data to the control station. Another approach uses a remote server station that connects to several cameras, with the server station coupling to a telephone line for reporting back to the control station. These and other recent implementations are directed to markets ranging from retail shops to large industrial warehouses.

Many other applications either cannot afford this expense or the applications for which they are targeted simply do not apply. Securing the confidentiality of electronically-displayed data is one such category of applications. This category includes maintaining the confidentiality of sensitive documents and data normally displayed on computer terminals, such as engineering documents, accounting data, strategic business plans, legal documents, medical records or any other information not intended for the casual onlooker.

Although unintentional, electronically displaying data openly on display terminals exposes a company to the risk of losing valuable commercial opportunities where safeguarding sensitive data is a requirement, such as in military contracts. A vendor that manages sensitive data daily as part of his core business, such as a credit reporting agency, also risks civil liability where an individual's personal data is stolen by a third party observing from behind a computer monitor user.

Finally, with the shift in the workplace from offices to cubicles or open floor plans, the personal privacy of the computer users in the workplace is becoming nonexistent. Data displayed for personal use is now easily visible to others as these new workplace designs typically have low walls and no doors to block the displayed information.

It would be highly desirable to have a security system for maintaining the confidentiality of electronically displayed information that does not require a substantial capital investment on the part of the security system user.

Summary of the Invention

The present invention is directed to a programmable electronic display arrangement and method and related needs for monitoring such displaying applications and environments, also referred to as display security. According to one example embodiment, a method and arrangement facilitate securing information electronically displayed on a display under the control of a display controller. The method includes detecting automatically a person within a predetermined range of the electronically displayed information, the person being in a position to view the electronically displayed information. A signal communicatively couples to the display controller in response to the automatic detection and, in response to the signal, the electronically displayed information is automatically blocked using the display controller.

A more specific implementation includes the above arrangement constructed and operating as part of a computer (display) terminal. The above circuit includes a sensing mechanism coupled to a small integrated circuit (IC) system board that interfaces with a display controller of the computer terminal. Detection software installed in the computer terminal configures the display controller to respond to the sensing mechanism by changing the displayed information upon detecting an unauthorized onlooker in front of the display.

Other aspects of the present invention are directed to example method and application-specific implementations relating to the above apparatuses.

The above summary is not intended to characterize each embodiment of the present invention. Other aspects of the present invention are provided by way of example upon review of the figures and corresponding description of the drawings.

Brief Description of the Drawings

Other aspects and advantages of the present invention will become apparent upon reading the following detailed description and upon reference to the drawings in which:

FIG. 1 illustrates an example office setting using an arrangement for securing electronically displayed information, according to an example embodiment of the present invention;

FIG. 2 is a block diagram of an example arrangement for securing electronically displayed information, according to an example embodiment of the present invention;

FIG. 3A is an example detection signal amplification circuit of an arrangement for securing electronically displayed information, according to the present invention;

FIG. 3B is an example keyboard microcontroller circuit of the arrangement for securing electronically displayed information, according to the present invention; and

FIG. 3C is an example media for storing a software application that operates with a display processor arrangement, according to the present invention.

While the invention is susceptible to various modifications in alternative forms, specific embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that it is not intended to limit the invention to a particular form disclosed. On the contrary, the invention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

Detailed Description

The present invention is applicable to secured and security-monitoring applications in which electronically displayed information is to be kept confidential

from casual onlookers. In one example implementation, a circuit arrangement interfaces with a display controller of a data processing system to automatically block information on a display terminal upon detecting a person that is within a predetermined range of the display terminal. For the purposes of this application, data processing systems include, but are not limited to, personal computers, internet appliances, servers, workstations, televisions, and portable digital devices, such as PDAs and mobile communication devices. While the present invention is not necessarily limited to such circuits and devices, an appreciation of various aspects of the invention is best gained through a discussion of various examples using this application.

According to an example embodiment of the present invention, a method for securing information electronically displayed on a computer display or monitor under the control of a display controller facilitates the protection of sensitive information from an onlooker that is within viewing range of the display. In a particular example, sensitive information that is displayed on a computer monitor is automatically blocked when a person is detected within a certain distance from the monitor. The display controller receives a signal alerting the display controller that a person is within viewing range and, in response to the signal, the display controller reconfigures the computer monitor to block the electronically displayed information. In this example, blocking of the information occurs upon reconfiguring the display to replace the sensitive information with either a screen saver application or with a blank screen.

In another example embodiment, a computer's display processor is reconfigured with a detection software application to respond to a detection module that detects unauthorized onlookers. The detection software application operates with the display

processor to provide a user with various display (or screen) blocking options from which to choose. In this particular example, the detection module includes a heat sensor that is coupled to a small IC (integrated circuit) printed circuit board, whereby the IC board is connected to the serial port or the keyboard port of the computer. When the heat sensor detects a person within a certain range of the screen, the IC board in conjunction with the detection software application signals a "trip" which enables the display controller to initiate one of the screen blocking options. As the heat sensor detects the person approaching the screen, the information displayed on the screen is blocked before he is able to read any of the information displayed.

Referring now to the figures, FIG. 1 illustrates an example office setting 100 using an arrangement for securing electronically displayed information, according to an example embodiment of the present invention. In this particular example, an office setting 100 that benefits from the security arrangement of the present invention includes a user 102 sitting at a desk 104 in front of a computer screen of a computer 106 that currently displays information for user 102. In this example, computer 106 is either located within an open cubicle 108 or located in an open work environment such that the information displayed on the computer screen is easily viewable by an onlooker such as a person 111.

In this example embodiment, computer 106 is communicatively coupled to a detection system 110 that detects or senses the presence of person 111 located behind or near user 102. Detection system 110 is configured to sense the presence of person 111 that crosses into a zone of detection, as illustrated by an imaginary circle or zone 114, that surrounds computer 106. Presumably, if person 111 is within zone 114 he can view

or read the information displayed on user's screen. As person 111 crosses into zone 114, detection system 110 transmits a trip signal to computer 106 indicating that someone is within zone 114. In response to the trip signal, computer 106 automatically blocks any electronically displayed information on the screen to prevent person 111 from viewing or reading the displayed information. In this example, blocking the displayed information includes, but is not necessarily limited to, replacing the displayed information with a screen saver or a blank screen.

In this example embodiment, detection system 110 is connected to computer 106 with a cable 112 via the computer's serial port, parallel port, I^2C bus or keyboard port. A detection software application accompanying system 110 reconfigures computer 106 to respond to detection system 110 and provide the user with various screen-blocking options. Depending on the type of sensing mode or mechanism used in detection system 110, the perimeter of zone 114 is configurable to meet the security needs of user 102. In addition, detection system 110 is configurable to process sensory data inputs that are in the form of heat, motion, light variations and sound, individually or in various combinations.

In another embodiment, an imaging device (not shown) is coupled to detection system 110 and captures images of person 111 crossing into zone 114 after being detected. The imaging device is configured to capture images at regular intervals or at a set time after the person crosses into the zone. The imaging device implemented with system 110 includes a video camera, a still photography camera, a frame grabber camera, a digital camera or infrared sensing equipment that provides images.

Alternatively, the imaging device is implemented using an analog camera having an NTSC/PAL decoder, such as the BT827 available from Brooktree, Inc.

In yet another example embodiment, a software application reconfigures computer 106 to provide a keystroke-tracking program. Once detection system 110 is tripped, the keystroke-tracking program is enabled and the keystrokes and/or system commands entered by an unauthorized person on the keyboard of computer 106 are automatically tracked and stored for later use. The sequence of keystrokes is later reviewable by user 102 by using the keystroke tracking program to determine the extent of the unauthorized person's access within computer 106 or access within the network to which the computer is connected.

FIG. 2 is a block diagram of an example security arrangement 200 for securing electronically displayed information, according to an example embodiment of the present invention. For the sake of brevity in the detailed description, elements in FIG. 2 that correspond to similar elements in FIG. 1 are not repeated or re-labeled. Differences between the figures are labeled with new reference numerals. In this particular example, security arrangement 200 includes a data processing system 201, which corresponds to computer 106, coupled to detection system 110. Data processing system 201 includes a display or screen 202, a data processing unit 204 and a data entry device 206. In this embodiment, data entry device 206 includes a keyboard. In a related embodiment, the data entry device includes a mouse or a stylus or the data entry device can be substituted with a touch screen version of screen 202 that facilitates data entry into data processing unit 204.

In this example embodiment, a detection module 220 is communicatively coupled to a serial port of data processing unit 204 via cable 112 (or via another communications path) and

is adapted to detect a person crossing into zone 114. In this example, detection module 220 is configurable to include at least one, or any combination thereof, of the following: a heat/infrared sensor, a motion detector, a sound detector and a light detector configured to detect variations in light. In another embodiment, detection module 220 includes an imaging device, such as a video camera, configured to simultaneously detect movement and capture images of a person crossing into zone 114.

Included with detection module 220 is a detection software application that is installed in a memory arrangement 204C. The software application reconfigures a display processor 204B that controls a display controller 204A such that various display blocking options are made available to user 102. With the display blocking options, user 102 configures display processor 204B to respond to detection module 220 by, for example, playing an audio file initially selected at set up by user 102 to alert the user of a person crossing into zone 114. In another example, display processor 204B responds to module 220 by instructing display controller 204A to launch a pre-selected program file that "paints over" the currently displayed information. In yet another example, the display processor instructs the display controller to drop the current screen display onto the tool bar, thereby displaying a blank screen or the operating system default screen.

In another embodiment, security arrangement 200 includes an optional detector adapter 222 configured to convert the different signals from the various sensing modes of detection module 220 into one signal for processing by the display processor. Optional detector adapter 222 provides arrangement 200 with the flexibility of using different sensors for different applications without reconfiguring the display processor to respond to a new sensor input. With adapter 222, the display processor need only respond to a single input irrespective of the

type of signal detected at module 220. In one example, detection module 220 detects the heat of a person crossing into zone 114 via a heat sensor. However, user 102 now wishes to reconfigure security arrangement 200 to sense motion instead of heat and thereby proceeds to change the sensing mode of module 220. Adapter 222 now automatically processes the "motion" signal input from module 220 and converts the signal for processing by the display processor. The signal conversion by adapter 222 is transparent to the display processor and obviates the need for user 102 to reconfigure the display processor.

In another embodiment, display processor 204B receives and stores additional data, which supplement the detection data already received from module 220, from an alternate media module 208 received from an input module 210. Input module 210 receives and decodes audio signals, video signals or both and transmits the decoded signals to alternate media module 208. In this embodiment, input module 210 includes either a microphone or a camera, or both, which are activated in response to a detection signal from detection module 220. Module 208 transmits the decoded signal to display processor for viewing on display 202 or for listening on a speaker (not shown). The decoded signals are also stored in memory arrangement 204C for a later security review by user 102. It will be appreciated that data processing unit 204 can be implemented to include a personal computer or a server.

In yet another related embodiment, detection module 220 is coupled to data processing unit 204 via a keyboard microcontroller circuit module (not shown). The keyboard circuit module is coupled to the keyboard port of data processing unit 204 and provides a separate keyboard port for keyboard 206. In this example, the keyboard microcontroller circuit module is configured to receive motion detection signals via detection module 220.

FIGs. 3A and 3B illustrate a detection signal amplification circuit 320 and a keyboard microcontroller circuit 330, respectively, can be used to implement detection module 220 of FIG. 2. Amplification circuit 320 (FIG. 3A) is configured to receive signals from a detection device, such as a motion sensor 322, upon detecting sound, heat, vibration, light variations and motion within zone 114. In this example embodiment, amplification circuit 320 receives a signal from sensor 322 and generates a signal at a sensor output port 324. Keyboard microcontroller circuit 330 (FIG. 3B) receives the signal from sensor output port 324 via a sensor input port 332 (FIG. 3B) and writes data to a keyboard data line via a keyboard input port 336 of the data processing unit. In response to the data signal from microcontroller circuit 330, the display processor signals the display controller to change the image currently displayed.

In a related embodiment, amplification circuit 320 is configurable to interface directly with display processor 204B of FIG. 2, via a port separate from the keyboard port, to change the image displayed.

In this example embodiment, amplification circuit 320 includes an input port 321 that receives a signal from motion sensor 322 upon sensing motion within zone 114. Motion sensor 322 (*e.g.*, an RE200B infrared pyroelectric sensor available from Glolab Corporation of Wappingers Falls, NY) generates an input signal at input port 321, which is implemented to include an RJ11 connector that receives the signal at pin 3 of the connector. The RJ11 connection provides the user the option of using a longer cable to place amplification circuit 320 and motion sensor 322 a desired distance away from data processing unit 204. Amplification circuit 320 amplifies the signal from sensor 322 and feeds the amplified signal into an integrated circuit (IC) 326 (*e.g.*, a one shot IC - LMC555 manufactured by National

Semiconductor of Santa Clara, CA). Integrated circuit 326 generates a clean, glitch-free signal or pulse that is the output signal at sensor output 324 and is the input signal at sensor input 332 of microcontroller circuit 330.

In this example embodiment, amplification circuit 320 includes a plurality of quad operational amplifiers 328A-328D (*e.g.*, a low power quad operational amplifier LM324 manufactured by National Semiconductor of Santa Clara, CA) which operate as signal amplifiers and window comparators. In this example, the detection signal is amplified by two identical and cascaded amplification stages. Amplification stage I includes a high pass filter feedback around amplifier 328B with the high pass filter utilizing a .1μF capacitor and a 2MEG resistor. The output of stage I drives a sensitivity tuning potentiometer 323 which feeds into stage II at amplifier 328C as a first input with a second input defined by a reference voltage via a voltage divider circuit comprising a set of 1MEG resistors 325A and 325B, respectively, in series with diodes 327A and 327B, respectively (*e.g.*, a diode 1N914 as manufactured by Fairchild Semiconductor of Portland, ME).

Window comparator 328A receives the output of stage II from amplifier 328C and a reference voltage and compares the two. Where the output of amplifier 328C is lower than the reference voltage, the output of comparator 328A is at Vcc and current does not flow through a resistor 329 (*e.g.*, 10K ohms) in series with a diode 327C. On the other hand, current flows through diode 327C and triggers integrated circuit 326 when the output of amplifier 328C is higher than the reference voltage at amplifier 328A. Window comparator 328B, similar to comparator 328A, also receives the output of stage II from amplifier 328C and a reference voltage and compares the two. Where the output of amplifier 328C is higher than the reference voltage, the output of comparator 328D is at Vcc and current does not flow through a diode

327D. On the other hand, current flows through diode 327D and triggers integrated circuit 326 when the output of amplifier 328C is lower than the reference voltage at comparator 328D. This type of circuit arrangement provides an upper and lower threshold for motion sensor 322 in determining the triggering point for integrated circuit 326. In addition, the DC gains used on amplifiers 328B and 328C determine the sensitivity of circuit 320 and, in many applications, are usually fixed at the factory to avoid modifications by the user.

Referring again to FIG. 3B, example keyboard microcontroller circuit 320 couples to the personal computer via a keyboard connector 336 and the computer's keyboard port. Circuit 330 also provides a keyboard port 338 that enables the user to plug (*e.g.*, via a 6-pin DIN connector) his keyboard into circuit 330 and daisy chain circuit 330 and the user's keyboard to the personal computer. Signals from the user's keyboard pass through circuit 330 transparently to the personal computer. Circuit 330 processes signals from amplification circuit 320 via an 8-bit microcontroller chip 334 (*e.g.*, a COP8SAA716M9 microcontroller manufactured by National Semiconductor) that interfaces with the computer via port 336. Controller 334 includes internal RAM and ROM circuits that eliminate the need for external memory or a boot circuit. In a related embodiment, circuit 330 includes a wireless interface module that provides a wireless connection with a wireless keyboard.

Keyboard inputs ports 336 and 338 use two signals, in addition to power and ground, to send data: a clock signal and a data signal. The user's computer provides the clock signal while the data signal is an open-collector signal that allows various sources to drive the signal. Controller 334 receives a signal from amplification circuit 320 at input port 332 (line 3) and writes data to the keyboard DATA line (line 14), which passes via a 3.9K resistor to pin 5 of ports 336 and 338. When the keyboard or the personal computer are using the keyboard DATA

line at the same time, controller 334 detects this condition and waits to transmit its data at a later time. Due to the open-collector nature of the DATA line, as a +5V signal is being transmitted on the line controller 334 detects when someone else is pulling the line down to ground. The display processor receives the signal from controller 334 and signals to the display controller that the image currently displayed needs to change because a person within viewing range of the display has been detected.

FIG. 3C is an example media 350 for storing a software application that operates with a display processor arrangement, according to the present invention. In this particular example, software application media 350 includes a compact disc read-only memory disc having thereon the detection software application. The software application is installed into computer 106 via a CD-ROM drive. In another embodiment, the software application is stored on a floppy disk. In yet another embodiment, the software application is stored on digital versatile disc read-only-memory disc.

The present invention has been described with reference to particular embodiments and particular applications. These embodiments and particular applications are only examples of the invention's usefulness and should not be taken as a limitation. Various adaptations and combinations of features of the embodiments and particular applications disclosed, and other applications that may benefit from the above architectures and system operations, are within the scope of the present invention.

Such embodiments and particular applications are examples only; the scope of the present invention is defined by the following claims.